TEERTHANKER MAHAVEER UNIVERSITY
Moradabad

# Title of E-Contents:
# Information Technology offences
# LCR 1004
# COURSE:-BA.LLB.BBA.LLB.B.COMLLB.

**Name of the creator: - Yogesh Chandra Gupta**
**Designation:-Asst. Prof. of Law**
**Department:-CLLS**

## UNIT:- ONE

## Information Technology Act, 2000: Salient Features and 2008 Amendments

### Salient features of Information Technology Act' 2000

Humans have always felt the need to better the existing technology and as the result of such a drive, technology has grown head over heels in the past few decades. This rapid growth in technology year after year paves way for further development in other fields. Thus, the development of the internet could be considered a milestone in all of human history. This expeditious and unpredictable growth of the internet and the technologies revolving it has raised numerous legal challenges on regulating and facilitating e-communication and commerce, for which different countries have adopted different methods of approach. The Information Technology Act, 2000 (–**the Act**l) and the features of IT Act 2000 - the first of its kind, was passed by the Parliament of India for providing sufficient legal infrastructure to e -commerce and further deals with cybercrimes and prescribes their respective punishments. The Act provides legal recognition to e-transactions, digital signatures, and other electronic means of communication. This Act also led to the amendment of the Indian Penal Code, 1860, the Indian Evidence Act, 1872 etc.

### Objective - Features of IT Act 2000

- With an increase in IT-enabled services, protection of private data and personal information of individuals have assumed massive importance in today‘s digital era. Taking a wider view, confidential and important information which is critical to the national security also necessitates protection. The IT Act provides the infrastructure which is needed to create a protective system and restrict access to that confidential information.
- The Model Law on Electronic Signatures was adopted by The United Nations Commission on International Trade Law (UNCITRAL) in 2001. The recommendations put forward by the general assembly urged all states to incorporate the said Model Law on Electronic Signatures into their own local laws. IT Law incorporates the said provisions on digital signatures and harmonizes with the UNICITRAL Model Law.
- Along with the advent of information technology, crimes have also made their way into the digital realm. Cybercrimes and e-commerce frauds like hacking, voyeurism,

identity theft, etc are becoming a growing concern all over the world. The IT Act defines these crimes and prescribes appropriate punishment to prevent such crimes.

- The Act also includes provisions for service providers to set up, maintain and upgrade computerized facilities while at the same time allowing them to collect and retain adequate service charges on being given due authorization from the State and Central Government.

**Salient Features of Information Technology Act**

- The IT Act extends to the whole of India.
- The Act has extra-territorial jurisdiction, i.e., the act applies to cyber offences committed outside India if a system or a network from India is involved in the said crime, irrespective of his/her nationality.
- Legally validates all e-contracts made through secure electronic channels.
- Legal framework for digital signatures by way of asymmetric cryptosystem and hash function has been included along with proper security measures for the same.
- Authentication has been given to electronic records.
- Provisions for establishing a Cyber Regulatory Appellant Tribunal and the procedure for the appointment of its adjudicating officers is finalized.
- Only an appeal to the High Court could be made against an order passed by the Cyber Regulatory Appellant Tribunal.
- Provisions for the appointment of the Controller of Certifying Authorities (CCA) has been included to regulate and license the working of the Certifying Authorities. The duty to act as a repository of all digital signatures lies with the Controller.
- The Act allows senior police officers and other officers to enter any public place and arrest without a warrant on crimes mentioned under this Act.
- Provisions for the constitution of a Cyber Regulations Advisory Committee are also included. The Committee is established with the aim to advise both the Central Government and the Controller.
- The Act defines and elaborates on various cyber crimes and contraventions, and prescribes their respective punishments.

- The provisions mentioned under this Act are not applicable to power of attorney, negotiable instruments, will, trust, and any contract for the sale of immovable property.
- The Act allows the state government to make rules to carry out the provisions of this act through a notification in the _Official Gazette‘.
- Enumerates on the offences done by companies.
- Elaborates on certain cases in which the services providers can be held liable

**Features of IT Act 2008 Amendment**

The IT Act witnessed major changes through its 2008 Amendment - (IT Act 2008 Amendment), which aimed at making itself technologically neutral. It was initiated at the Parliament to address certain drawbacks and deficiencies the original Act faced. The new changes brought by the amendment hopes to help the Act accommodate future development of IT and related security concerns in this dynamic sector. It further includes several provisions relating to data protection and privacy. Here are some of the major changes

- **Incorporation of Electronic Signature:** To go by their aim of making the act _technologically neutral, the term _digital signature‘ has been replaced with _electronic signature‘, as the latter represents an umbrella term which encompasses many different types of digital marketing, while the former is a specific type of electronic signature.
- **Fight against Cyber-terrorism:** Pursuant to the 26/11 Mumbai Attacks, the amendment has incorporated the concept of cyber terrorism and prescribed hefty punishments for it. The scope of cybercrime under Section 66 is widened with many major additions defining various cybercrimes along with the controversial Section 66A which penalized sending ‑offensive messages‖. Section 66A was later found to be in violation of one‘s fundamental right to freedom of speech and expression and thus was struck down.
- **Child Pornography:** Along with reducing the term of imprisonment and increasing the fine for publishing obscene material in electronic form, an array of sections have also been inserted under Section 67, one among which recognizes publishing child pornography as a felonious act.

- **Cyber Cafes:** Cybercrimes like sending obscene e-mails to harass individuals, identity theft, and maliciously acquiring net banking passwords have many at times been taking place at Cyber Cafes. Due to the lack of inclusion of _Cyber Cafes‘ in the IT Act, they are incapable of being regulated. The 2008 amendment explicitly defines them and includes them under the term _intermediaries‘, thus allowing several aspects of the Act to be applicable to them.
- **Government Interception and Monitoring:** The new amendment allows the government to listen in to your phone calls, read your SMS‘s and emails, and monitor the websites you visit without getting a warrant from a magistrate. The same clause under the Telegraph Act was restricted by the condition of public emergency or safety, but the new amendment drops all such restrictions, vastly extending the government‘s power.

## Conclusion

The Information Technology (Amendment) Act, 2008 was passed to overcome some inherent shortcomings of the original Act and with the goal to tackle various challenges in the cyber world. Even though the 2008 amendment did manage to close the gap a little, there are still many problems which are evident. The problems with this legislation could be traced back to certain inadequacies like t he amendment reducing the magnitude of punishment for certain cybercrimes, allowing those cybercrimes to remain bailable, the omission of crimes committed through mobile phones and the complete exclusion of the concept of cyberwar. It is only expected that a single amendment cannot cover all shortcomings of an act, especially when the subject matter is as dynamic as information technology. As the horizons of technology widen, more amendments will be needed to tackle the existing and future shortcomings in order to create a satisfactory, well laid-out framework which along with its plethora of goals, deters cybercriminals.

**UNIT: - TWO**

**The Cyber Appellate Tribunal**

**Table of Contents**



## Introduction

Computers, the Internet, and ICT, or e-revolution, have transformed people's lives in the twenty-first century. E-communication has mostly replaced paper-based communication in recent years. As a result, new terms like the cyber world, e-transaction, e-banking, e-return, and e-contracts have emerged. Aside from the good aspects of the e-revolution, there is also a bad aspect of computers, namely, the internet and ICT in the hands of criminals, which has turned into a weapon of crime. As a result, a new panel of members, known as Cyber Law, Cyber Space Law, Information Technology Law, or Internet Law, was formed to address the issues of cybercrime in cyberspace.

Cyber legislation and the Information Technology Act of 2000, as amended in 2008, are being developed in India to combat computer crimes. The Information Technology Act of 2000 is a law that establishes legal recognition for transactions carried out via Electronic Data Interchange (EDI) and other forms of electronic communication. It is India's principal legislation governing cybercrime and electronic trade (e-Commerce). Electronic data interchange or electronic filing of the information is referred to as e-Commerce.

The Information Technology Act of 2000, which took effect on October 17, 2000, was enacted to *provide legal recognition for transactions carried out through electronic data interchange and other forms of electronic communication, also known as "electronic commerce,"* involve the use of alternatives to *paper-based methods of communication and information storage, to make* electronic filing of documents with government agencies easier, and to amend the Information Technology Act of 2000.

The Internet network has vastly grown over vast geographic distances, allowing for fast communication between even the most remote parts of the globe. Various global institutions see the need for rules to regulate this new hemisphere as human activities in this limitless new universe continues to expand. The Information Technology (IT) Act 2000 was established in India to keep up with the continuous flux. The IT Act was conceived and formed according to the Model Law of the United Nations Commission on International Trade Law (UNCITRAL).

*The Cyber Appellant Tribunal was created under the Information Act of 2000. The tribunal solely has appellant jurisdiction, as its name implies. As a result, it has the ability to exercise its appellant jurisdiction over a judgment or order made by the Controller of Certifying Authorities or the adjudicating official, both on the facts and in law. In other words, it has the legal authority to investigate the decision or order's accuracy, legality, and propriety. The Central Government has created the country's first and only Cyber Appellate Tribunal in line with the terms of Section 48(1) of the Information Technology Act, 2000.*

**Establishment of the Tribunal (Section 48)**

This Section explains how the Cyber Appellant Tribunal will be established. The central government will issue a notification establishing one or more appellant tribunals. The Central Government also lists all of the subjects and locations that come under the Tribunal's jurisdiction in the announcement.

**Composition (Section 49)**

This Section explains that the Presiding Officer of the Cyber Appellate Tribunal, who will be nominated by the Central Government, will be the sole member of the Cyber Appellate Tribunal. The appellant tribunal has been transformed into a multi-member body. The Tribunal will henceforth be composed of *a Chairperson* and as *many additional members as the Central Government may designate by publication in the Official Gazette*. The Central Government, in collaboration with the Chief Justice of India, selects the Chairperson and Members of the Tribunal. The Tribunal's Presiding Officer is now known as the Chairperson.

**Power and procedure of the Cyber Appellant Tribunal (Section 58)**

The Cyber Appellate Tribunal's method and powers are laid forth in Section 58 of the Information Technology Act, 2000

Sub-clause (1) Section 58 states that the Cyber Appellate Tribunal is not bound by the Code of Civil Procedure, 1908, but rather by the principles of natural justice and that the Cyber Appellate Tribunal, subject to the other provisions of this Act and any rules, has the authority to regulate its own procedure, including the location of its hearings.
Clause (2) Section 58 stipulates that, for the purposes of executing its responsibilities under this Act, the Cyber Appellate Tribunal shall have the same powers as a civil court under the Code of Civil Procedure, 1908, while trying an action, in respect of the following matters:

(a) Summoning and enforcing the attendance of any person and examining him on oath;

(b) Requiring the discovery and production of documents or other electronic records;

(c) Receiving evidence on affidavits;

(d) Issuing commissions for the examination of witnesses or documents;

(e) Reviewing its decisions;

(f) Dismissing an application for default or deciding it ex parte;

(g) Any other matter which may be prescribed.

Clause (3) Section 58 states that any proceeding before the Cyber Appellate Tribunal is deemed to be a judicial proceeding for the purposes of Sections 193 and 228 of the Indian Penal Code, and the Cyber Appellate Tribunal is deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

In ***Union of India v. T. R. Verma***, It is claimed that it is established law that courts must observe the law of natural justice, which states that a party must be given the chance to present any relevant evidence on which he relies. Evidence should be taken in the presence of the parties, and cross-questioning should be allowed.

**Limitation (Section 60)**

The limitations restrictions of the Limitation Act of 1963 apply to Tribunal appeals.

**Civil Court not to have jurisdiction (Section 61)**

Section – No civil court can consider a suit or action in that area if the IT Act of 2000 authorizes the adjudicating officer or the Cyber Appellate Tribunal to deal with particular concerns.

Furthermore, no court can issue an injunction against any conduct taken by a person in the exercise of any authority conferred by the Act.

**Appeal to the High Court (Section 62)**

Section – A person aggrieved by the CAT's decision or order may submit an appeal to the HC *within sixty days of the date of notification of the Tribunal's decision* or order to him on any point of fact or law arising out of such order, according to Section 62 of the IT Act. The HC may if satisfied that the appellant was prevented from submitting the appeal within the specified term by sufficient cause, allow it to be submitted within an additional period of not more *than sixty days*.

**Recovery of Penalty (Section 64)**

If a penalty issued under this Act is not paid, it is collected as land revenue arrears. Furthermore, until the penalty is paid, the license or digital signature certificate is suspended.

**Conclusion**

The purpose of enacting the I.T. Act was straightforward. The government wanted to offer and support electronic, digital transactions while also safeguarding against all types of cybercrime. Because of the quantity of traffic on the internet and the amount of money individuals transact through online means, it was critical to strengthen the cyber world. Although the cyber world is vastly different from the actual world, it has the capability to participate in crimes that occur in the real world. The Cyber Appellant Tribunal was created to combat cybercrime and punish individuals involved. The effectiveness of the Cyber Appellant Tribunal may be improved by increasing public and government knowledge, as well as attempts to deploy enough staff. It is critical to improving technical capability in order to deal with any circumstance that may arise. Integrity, secrecy, and authenticity of communication routes and procedures are required.

Certain sorts of offenses necessitate the use of tribunals that can make decisions more quickly. The judgment is likely to be made quickly if it follows the natural justice system rather than the C.P.C. In ***M/s. Gujarat Petrosynthese Ltd. and Mr. Rajendra Prasad Yadav v. Union of India*** it sought for a direction to the Respondent to designate a Chairperson to the Cyber Appellate Tribunal (CAT) in order to guarantee that the tribunal's hearings were convened on a regular basis. In court, it was said that the department would take all necessary steps to fill the position of chairman within the time limit of six months, and that attempts would be made to appoint the

chairperson even before the time limit expired, in the public interest. On these grounds, the petition was dismissed. Despite the above judgment, no appointment to the cyber appellate tribunal has been made as of yet, and it has been inactive since 2011.

# UNIT:- THREE
# Offences under IT Act, 2000

## INTRODUCTION

The introduction of the internet has brought tremendous changes to our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for the sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offenses led to the need for a law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian parliament passed the law – **Information Technology Act**, 2000. The **IT Act 2000** has been conceptualized on the **United Nations Commissions on International Trade Law** (UNCITRAL) model law.

The Government of India enacted its **Information Technology Act,** 2000 with the objectives stating officially as: ‑to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‑electronic commerce‖, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the **Indian Penal Code,** the **Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934** and for matters connected therewith or incidental thereto.‖

## CYBERCRIME

Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyberspace and the worldwide web. Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Net crime is criminal exploitation of the Internet.

The offenses included in the IT Act 2000 are as follows**:**

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.

4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offense or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offenses.

**Offenses UNDER THE IT ACT, 2000**

**1. Tampering with computer source documents:**

Section 65 of this Act provides that Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer Programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

**Explanation:**

For the purpose of this section –computer source code‖ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

**Object:**

The object of the section is to protect the –intellectual property‖ invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

This section extends towards the Copyright Act and helps the companies to protect the source code of their programmes.

**Section 65** is tried by any magistrate. This is cognizable and non- bailable offense.

Imprisonment up to 3 years and or Fine up to Two lakh rupees.

**CASE LAWS**

***Frios v. State of Kerela***

**Facts:** In this case, it was declared that the FRIENDS application software as a protected system. The author of the application challenged the notification and the constitutional validity of software under **Section 70**. The court upheld the validity of both.It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

**Held:** The court held that Tampering with Source code is punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

***Syed Asifuddin case***

**Facts:** In this case, the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.

**Held:** Court held that Tampering with source code invokes **Section 65** of the **Information Technology Act**.

***Parliament Attack Case*:**

**Facts:** In this case, several terrorists attacked Parliament House on 13 December 2001. In this Case, the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence, should not be relied. In Parliament case, several smart device storage disks and devices, a Laptop was recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V news channels. In this case design of Ministry of Home Affairs car sticker, there was game ‑wolf pack‖ with user name of _Ashiq', there was the name in one of the fake identity cards used by the terrorist. No back up was taken. Therefore, it was challenged in the Court.

**Held:** Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

**2. Hacking with the computer system:**

**Section 66** provides that- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation: The section tells about the hacking activity.

Punishment: Imprisoned up to three years and fine which may extend up to two lakh rupees Or with both

**CASE LAWS**

***R v. Gold & Schifreen***

In this case, it is observed that the accused gained access to the British telecom Prestl Gold computers networks file amount to dishonest trick and not a criminal offense.

***R v. Whiteley***

In this case, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users. The perspective of the section does not merely protect the information but to protect the integrity and security of computer resources from attacks by unauthorized person seeking to enter such resource, whatever may be the intention or motive.

**Cases Reported In India:**

Official website of Maharastra government hacked. The official website of the government of Maharashtra was hacked by Hackers Cool Al- Jazeera, and claimed them they were from Saudi Arabia.

**3. Publishing of obscene information in electronic form:**

**Section 67** of this Act provides that Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

**CASE LAWS:**

***The State of Tamil Nadu v. Suhas Katti.***

**Facts:** This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. These

postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through the internet.

**Held:** The accused is found guilty of offenses under **section 469, 509 IPC** and **67 of the IT Act 2000** and the accused is convicted and is sentenced for the offense to undergo RI for 2 years under **469 IPC** and to pay fine of Rs.500/-and for the offense u/s **509 IPC** sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offense **u/s 67** of **IT Act 2000** to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently. The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under **section 67** of **Information Technology Act 2000** in India.

In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

***Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies)*** **case.**

**Facts:** There were three accused first is the Delhi schoolboy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were **Section 292** (sale, distribution, public exhibition, etc., of an obscene object) and **Section 294** (obscene acts, songs, etc., in a public place) of the **Indian Penal Code** (IPC), and **Section 67** (publishing information which is obscene in electronic form) of the **Information Technology Act 2000**. In addition, the schoolboy faces a charge under **Section 201** of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offenses invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first-time conviction, and/or fines.

**Held:** In this case, the Service provider Avnish Bajaj was later acquitted and the Delhi schoolboy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

**4. Power of Controller to give directions:**

**Section 68** of this Act provides that (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such

activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

***Explanation:*** Any person who fails to comply with any order under subsection (1) of the above section, shall be guilty of an offense and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The offense under this section is non-bailable & cognizable.

Punishment: Imprisonment up to a term not exceeding three years or fine not exceeding two lakh rupees.

**5. Directions of Controller to a subscriber to extend facilities to decrypt information:**

**Section 69** provides that- (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offense; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in subsection shall be punished with imprisonment for a term which may extend to seven years. Punishment: Imprisonment for a term which may extend to seven years. The offense is cognizable and non- bailable.

**6. Protected System:**

**Section 70** of this Act provides that –

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

***Explanation:*** This section grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

Punishment: The imprisonment which may extend to ten years and fine.

**7. Penalty for misrepresentation:**

**Section 71** provides that- (1) Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Punishment: Imprisonment which may extend to two years or fine may extend to one lakh rupees or with both.

**8. Penalty for breach of confidentiality and privacy:**

**Section 72** provides that- Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made thereunder, has secured assess to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

***Explanation:*** This section relates to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations have secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such a person discloses such information, he will be punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Punishment: Term which may extend to two years or fine up to one lakh rupees or with both.

**9. Penalty for publishing Digital Signature Certificate false in certain particulars:**

**Section 73** provides that – (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-

(a) The Certifying Authority listed in the certificate has not issued it; or

(b) The subscriber listed in the certificate has not accepted it; or

(c) The certificate has been revoked or suspended unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with

imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

***Explanation:*** The Certifying Authority listed in the certificate has not issued it or, The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation, the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offense it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Punishment: Imprisonment of a term of which may extend to two Years or fine may extend to 1 lakh rupees or with both.

**CASE LAWS:**

***Bennett Coleman & Co. v. Union of India***

In this case, the publication has been stated that _publication means dissemination and circulation'. In the context of the digital medium, the term publication includes and transmission of information or data in electronic form.

**10. Publication for fraudulent purpose:**

**Section 74** provides that- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extends to one lakh rupees, or with both.

***Explanation:*** This section prescribes punishment for the following acts:

Knowingly creating a digital signature certificate for any

1. fraudulent purpose or,
2. unlawful purpose.

Knowingly publishing a digital signature certificate for any

1. fraudulent purpose or
2. unlawful purpose

Knowingly making available a digital signature certificate for any

1. fraudulent purpose or
2. unlawful purpose.

Punishment: Imprisonment for a term up to two years or fine up to one lakh or both.

**11. Act to apply for offense or contravention committed outside India:**

**Section 75** provides that- (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offense or contravention committed outside India by any person irrespective of his nationality.

For the purposes of sub-section (1), this Act shall apply to an offense or Contravention committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India.

***Explanation:*** This section has a broader perspective including cyber crime, committed by cyber criminals, of any nationality, any territoriality.

**CASE LAW:**

***R v. Governor of Brixton prison and another***

**Facts**: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account into the accounts of the hacker, later identified as Valdimer Levin and his accomplices. After Levin was arrested he was extradited to the United States. One of the most important issues was the jurisdictional issue, the _place of origin' of cyber crime.

**Held:** The Court held that the real-time nature of the communication link between Levin and Citibank computer meant that Levin's keystrokes were actually occurring on the Citibank computer. It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.

**12. Confiscation:**

**Section 76** provides that- Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation. :

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made

thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

***Explanation:*** The aforesaid section highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

**13. Penalties or confiscation not to interfere with other punishments:**

**Section 77** provides that – No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

***Explanation:*** The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

**Power to investigate offenses:**

**Section 78** provides that – Notwithstanding anything contained in the **Code of Criminal Procedure, 1973**, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offense under this Act.

**CONCLUSION**

Due to the increase in digital technology, various offenses are increasing day by day. Therefore, the IT Act 2000 need to be amended in order to include those offenses which are now not included in the Act. In India, cybercrime is not of high rate. Therefore, we have time in order to tighten the cyber laws and include the offenses which are now not included in the IT Act 2000.

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This has led to tremendous development and progress which has been a launching pad for further developments. Of all the significant advances made by mankind from the beginning to date, probably the most important of them is the development of the Internet.

However, the rapid evolution of the Internet has also raised numerous legal issues and questions. As the scenario continues to be still not clear, countries throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication and commerce.

**Cyber Stalking:**

In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

***How do Cyber Stalkers operate?***

1. They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.
2. The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.
3. People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.
4. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.
5. Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
6. In online stalking the stalker can make third party to harass the victim.
7. Follow their victim from board to board. They –hangoutǁ on the same BB‘s as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will –flameǁ their victim (becoming argumentative, insulting) to get their attention.

8. Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.
9. Contact victim via telephone. If the stalker is able to access the victim's telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.
10. Track the victim to his/her home.

**Mail spoofing**

**Introduction**

Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a known sender. The goal of email spoofing is to trick recipients into opening or responding to the message.

The most commonly accepted email spoofing definition is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email. This way, the protocols think it came the real sender.

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.

Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages.

Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged

**How Email Spoofing Works**

The goal of spoofing is to trick users into believing the email is from someone they know or can trust—in most cases, a colleague, vendor or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.

For example, an attacker might create an email that looks like it comes from PayPal. The message tells the user that their account will be suspended if they don't click a link, authenticate into the site and change the account's password. If the user is successfully tricked and types in credentials, the attacker now has credentials to authenticate into the targeted user's PayPal account, potentially stealing money from the user.

More complex attacks target financial employees and use social engineering and online reconnaissance to trick a targeted user into sending millions to an attacker's bank account. To the user, a spoofed email message looks legitimate, and many attackers will take elements from the official website to make the message more believable.

**Reasons for email spoofing**

In addition to phishing, attackers use spoofed email for the following reasons:

- Hide the fake sender's real identity.
- Bypass spam filters and blocklists. Users can minimize this threat by blocklisting internet service providers (ISPs) and Internet Protocol (IP) addresses.
- Pretend to be a trusted individual -- a colleague or a friend -- to elicit confidential information.
- Pretend to be a reliable organization -- for example, posing as a financial firm to get access to credit card data.
- Commit identity theft by impersonating a targeted victim and requesting personally identifiable information (PII).
- Damage the sender's reputation.
- Launch and spread malware hidden in attachments.
- Conduct a man-in-the-middle (MitM) attack to seize sensitive data from individuals and organizations.
- Obtain access to sensitive data collected by third-party vendors

**Ways to stop email spoofing**

Users and businesses can prevent email spoofers from accessing their systems in a variety of ways.

**1. Deploy an email security gateway**

Email security gateways protect businesses by blocking inbound and outbound emails that have suspicious elements or do not meet security policies a business puts in place. Some gateways offer additional functions, but all can detect most malware, spam and phishing attacks.

**2. Use antimalware software**

Software programs can identify and block suspicious websites, detect spoofing attacks and stop fraudulent emails before they reach user inboxes.

**3. Use encryption to protect emails**

An email signing certificate encrypts emails, allowing only the intended recipient to access the content. In asymmetric encryption, a public key encrypts the email, and a private key owned by the recipient then decrypts the message. An additional digital signature can ensure the receiver that the sender is a valid source. In environments without broad encryption in place, users can learn to encrypt email attachments.

**4. Use email security protocols**

Infrastructure-based email security protocols can reduce threats and spam by using domain authentication. In addition to SMTP and SPF, businesses can use DomainKeys Identified Mail (DKIM) to provide another layer of security with a digital signature. Domain-based Message Authentication, Reporting and Conformance (DMARC) can also be implemented to define the actions that should be taken when messages fail under SPF and DKIM.

**5. Use reverse IP lookups to authenticate senders**

A reverse IP lookup confirms the apparent sender is the real one and verifies the email's source by identifying the domain name associated with the IP address.

Website owners can also consider publishing a domain name system (DNS) record stating who can send emails on their domain's behalf. Messages are then inspected before the email body is downloaded and can be rejected before causing any harm.

**6. Train employees in cyber awareness**

On top of software-based anti-spoofing measures, businesses must encourage user caution, teaching employees about cyber security and how to recognize suspicious elements and protect themselves. Simple educational programs can equip users with email spoofing examples and give them the ability to spot and handle spoofing tactics, along with procedures to follow when a spoofing attempt is discovered. Training should be ongoing so that the materials and methods can be updated as new threats emerge.

**7. Watch out for possible spoofed email addresses**

The email addresses users communicate with are often predictable and familiar. Individuals can learn to watch out for unknown or odd email addresses and to verify an email's origin before interacting with it. Attackers often use the same tactics multiple times, so users must remain vigilant.

**8. Never give out personal information**

In many situations, even if spoofed emails get into an inbox, they only cause real damage when a user responds with personal information. By making it a common practice never to divulge personal information in emails, users can significantly limit the effects email spoofing could have.

**9. Avoid strange attachments or unfamiliar links**

Users should also steer clear of suspicious attachments and links. As a best practice, they can examine every element of an email, looking out for telltale signs, like misspellings and unfamiliar file extensions, before going ahead and opening a link or attachment.

## UNIT FOUR

**QUEST: - DISCUSS THE APPOINTMENT AND FUNCTION OF CONTROLLER**

**ANS:-Controller under Information Technology Act**

The provisions of appointment and functions of the controller are given under sections 17 and 18 of chapter 6 of _Information Technology Act, 2000. (Words _other officer' and employees is enforced in section 17 after _Information Technology' (Amendment) Act, 2008). For the purpose of this Act Controller, Deputy Controller, and Assistant controller are known as certifying authorities.

**Section 11: Appointment of the controller and other officers-**The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification, appoint a such number of Deputy Controllers, Assistant Controllers, other officers and employees as it deems fit. (Sub-section 1).

Sub-section (4) qualifications, experience and terms, and conditions of service of Controller, Deputy Controllers, Assistance Controllers, other officers, and employees shall be such as may be prescribed by the Central Government.

**Subordination-**According to sub-section (2), the Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

Same as according to sub-section (3), The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

**Head Office-**The Head Office and Branch Office of the office of the Controller shall be at such places at the Central Government may think fit. (Sub-section 5)

**Seal-**Sub-Section (6) there shall be a seal of the Office of the Controller. Such as section 17 has provisions regarding the appointment of Controller, Deputy Controller, and Assistant controller as certifying authorities and they are subordinates. Head office and seal. The appointment of certifying authorities is presented-

- Certifying Authorities
- Central Govt. (Appoint mentor)
- Controller
- Deputy Controller
- Assistant Controller

**Section 18 describes the functions of Controller, they are following-**

**Functions of Controller-**The Controller may perform all or any of the following functions, namely-

1. Exercising supervision over the activities of the Certifying Authorities;
2. Certifying public keys of the certifying Authorities.
3. Laying down the standards to be maintained by the Certifying Authorities;
4. Specifying the qualifications and experience which employees of the Certifying Authority should possess;
5. Specifying the conditions subject to which the Certifying Authorities shall conduct their business;
6. Specifying the contents of written, printed, or visual materials and advertisements that may be disturbed or used in respect of an Electronic Signature Certificate and the public key.
7. Specifying the form and contents of an (electronic signature) Certificate and the key;
8. Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
9. Specifying the terms and conditions and subject to which auditors may be appointed and the remuneration to be paid to them;
10. Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulations of such systems;
11. Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.
12. Resolving any conflicts of interests between the Certifying Authorities and the subscribers;
13. Laying down the duties of the Certifying Authorities;
14. Maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to the public.

**QUEST: - BREACH OF CONFIDENTIALITY AND PRIVACY**

**ANS: -** Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be legally protected). The law does not determine what privacy is, but only what situations of privacy will be afforded legal

protection. It is interesting to note that the common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one.

The meaning of the word confidentiality and privacy are somewhat synonymous. Confidentiality involves a sense of 'expressed or 'implied basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Right to privacy is more of an implied obligation. It is the 'right to let alone.

In the legal parlance the issue of confidentiality comes up where an obligation of confidence arises between a 'data collector and a 'data subject. This may flow from a variety of circumstances or in relation to different types of information, which could be employment, medical or financial information. An obligation of confidence gives the data subject the right not to have his information used for other purposes or disclosed without his permission unless there are other overriding reasons in the public interest for this to happen.

That is, where an information for a purpose other than that for which it was provided. Hence right is an interest recognized and protected by moral or legal rules. It is an interest, the violation of which would be a legal wrong. Respect for such interest would be a legal duty. It is the basic principle of jurisprudence that every right has a correlative duty and every duty has a correlative right. But the rule is not absolute. It is subject to certain exceptions in the sense that a person may have a right but there may not be a correlative duty. Nevertheless, it would be prudent if the issues related to privacy (and confidentiality) are viewed as 'rights along with duties.

**What is a privacy policy?**

A privacy policy is a legal document that discloses the way a party gathers, uses, discloses, and manages a customer or client‘s data. It fulfills a legal requirement to protect a customer or client‘s privacy.

Such privacy policy must provide the following:

1. clearly and easily accessible statements of its practices and policies;
2. clearly state the type of personal and sensitive personal data or information collected by the business;
3. purpose of collection and usage of such information;
4. about disclosure of information including sensitive personal data or information collected; and
5. Reasonable security practices and procedures adopted by it

**Penalty for the Breach of Confidentiality and Privacy under the act**

**Section 72 of the Information Technology act, 2000** doesn't specify the provision relating to the breach of privacy by the data processor but talks about a circumstance under which any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, such person shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000 or with both.

**Section 72 of the Act relates to any person who, in pursuance of any of the powers conferred by the Act or its allied rules and regulations has secured access to any:**

I. Electronic record,
II. book,
Register,
III. Correspondence,
IV. Information,
V. Document, or
VI. Other material.

If such person discloses such electronic record, book, register, correspondence, information, document or other material to any other person, he will be punished with imprisonment for a term, which may extend to two years, or with fine, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

This section applies only to person who has gained access to the abovementioned information in pursuance to a power granted under Information Technology Act, its allied rules e.g. a police officer, the Controller etc. it would not apply to disclosure of personal information of a person by a website, by his email service provider etc.

**Persons conferred with power under the Act**

the Act has conferred powers to:

- The Controller of Certifying Authorities (Ss. 17-18)
- The Deputy and Assistant Controllers of Certifying Authorities (Ss. 17 and 27)
- Licensed Certifying Authorities (S. 31) and Auditors (Rule 312)
- The Adjudicating Officer (S 46)

- The Presiding Officer of the Cyber Appellate Tribunal (Ss. 48-49)
- The Registrar of the cyber Appellate tribunal (S. 56 and rule 263)
- Network Service provider (S. 79)

**Provision of breach of confidentiality and privacy under IT Act 2000**

Section 43 of the Act covers instances such as

I. Computer trespass, violation of privacy etc.
II. Unauthorized digital copying, downloading and extraction of data, computer database or information;. theft of data held or stored in any media,
III. unauthorized transmission of data or programme residing within a computer, computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible),
IV. data loss, data corruption etc.,
V. computer data/database disruption, spamming etc.,
VI. denial of service attacks, data theft, fraud, forgery etc.,
VII. unauthorized access to computer data/computer databases and
VIII. Instances of data theft (passwords, login IDs) etc.

The Information Technology Act, 2000 provides for civil liability in case of data, computer database theft, privacy violation etc. The Act also provides a complete Chapter (Chapter XI) on cyber offences, i.e., sections 65-74 which cover a wide range of cyber offences, including offences related to unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, and computer database. For example, section 65 [Tampering with computer source documents] of the Act is not limited to protecting computer source code only, but it also safeguards data and computer databases; and similarly section 66 [Hacking with Computer System] covers cyber offences related to (a) Illegal access, (b) Illegal interception, (c) Data interference, (d) System interference, (e) Misuse of devices, etc. The Information Technology Act, 2000 provides for criminal liability in case of data, computer database theft, privacy violation etc.

**QUEST: - EXTRA TERRITORIAL JURISDICTION FOR CYBER CRIMES IN INDIA**

**ANS:-** Under the Indian criminal justice system, jurisdiction is conferred upon domestic Courts to conduct trials for offences committed within India and also certain offences committed outside Indian territory. Sections 3 and 4 of the Indian Penal Code, 1860 (**–IPC**‖) specify certain

situations where trial can be conducted in India, for offences committed abroad. The Code of Criminal Procedure, 1973 (**–CrPC**‖) prescribes the procedure which must be followed before trials can be initiated in India, for offences committed outside Indian Territory. In so far as offences committed abroad which target a computer resource are concerned, Indian Courts are said to possess jurisdiction if the computer resource targeted is located in India.

The Information Technology Act, 2000 (**—IT Act**‖) which provides the legal framework for regulating activities in cyberspace, also defines various offences and prescribes penalties for the same. If any such offence under the IT Act is committed within Indian territory, Indian Courts would have jurisdiction to conduct a trial as per the procedure under the CrPC. Further, similar to the treatment of offences committed against computer resources under IPC, under Section 75 of the IT Act also, Indian Courts have jurisdiction to try cyber offences, only if the computer, computer system or computer network (which are all covered within the broader definition of _computer resource') involved in the commission of the offence is/are located in India. While Section 75 also deals with _contraventions' of the IT Act committed outside the territory of India, the purpose of this article is limited to its relevance in determining jurisdiction of criminal Courts.

A study of this arrangement (both under the IPC and IT Act) for conferring jurisdiction upon Indian Courts in cases of cyber offences committed abroad, along with a general study of relevant provisions of the CrPC, suggests that the current arrangement appears to be redundant and not serving any purpose. The present article aims to critique this arrangement and highlight the existing redundancy

**Applicability and Jurisdiction of the IT Act**

The Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. If a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India? According to Sec.1 (2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further, Sec.75 of the IT Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**Cross border jurisdiction for offences under it act**

The IT Act has separate chapters on contraventions and offences, respectively, which are specifically defined and punishable. Section 75 of the IT Act confers cross-border jurisdiction on Indian Courts, to try offences or contraventions under the IT Act, committed outside the territory of India. However, such jurisdiction is limited to cases where the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

The abovementioned provision, in spite of being very similar to Section 4(3), IPC, is broader in scope, as it grants jurisdiction to Indian Courts for trying offences committed abroad which involve a computer, computer system or computer network located in India, and not just where the computer resource targeted is located in India (which is the case under the IPC). Hence, for offences under the IT Act, jurisdiction may be assumed by Indian Courts for offences committed abroad if any of the computer resources (and not just the resource targeted) involved in an offence, are located in India

**Section 75. Act to apply for offence or contravention committed outside India.**

(1) Subject to the provisions of sub-section *(2)*, the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

---

(2) For the purposes of sub-section *(1)*, this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**Quest: - Digital Signatures- What is Digital Signatures?**

**Ans:-** The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature. The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

The Information Technology Act, 2000 includes provisions for the use of Digital Signatures on documents which are submitted in electronic form with the objective of maintaining

security and authenticity of the documents filed online. A digital signature certificate (DSC) which is issued by a certifying authority is a digital key that authenticates identity of individuals and businesses holding the certificate.

It is possible to create the digital signature certificate online and apply it to online documents. The DSC has successfully replaced physical signature. It can be created and obtained from digital signature certificate providers. Verasys Technologies, a subsidiary company of Alankit Limited is a leading service provider for digital signatures. The company facilitates the digital signature application & related procedures and issues digital signatures based on Aadhaar e-KYC in an extremely convenient manner.

**Meaning of Digital Signature – Information Technology Act, 2000**

Digital signature is a mathematical scheme to verify the authenticity of digital documents or messages. Digital Signature under Information Technology Act, 2000 is primary law in India dealing with cyber crime and e-commerce. According to the Information Technology Act, 2000, digital signatures mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. Further, the IT Act, 2000 deals with digital signatures under sections 2, 3 and 15

**What is the Purpose of a Digital Signature?**

Digital signature is an indispensable part of electronic commerce, where customers, vendors, and suppliers can sign important documents electronically. Not just e-commerce, but the digital signature is widely used in authentication schemes across different sectors. Digital signature authenticates the identity of individuals sending any document digitally. E-signatures bring with them legal validity and also ensures security. Digital signatures are among the most important components of an e-signature program and can drive security and legal validity. It is also important for record management, and people across different sectors rely on e-signature.

**How are digital signatures created?**

A digital signature is created using hash algorithms or a scheme of algorithms like DSA and RSA that use public key and private key encryptions. The sender uses the private key to sign the message digest (not the data), and when they do, it forms a digital thumbprint to send the data.

It's important to note here that all the tools used to **digitally sign** a document are numerical in nature. Digital signature solutions use crypto-algorithms to convert both the document to be signed and the private key (which is already in character form), into a new set of

encrypted characters.

When a signed document is authenticated using the public key, the signer is aware of who created it & whether the document has been altered since being digitally signed. The decryption process gets back the original hashed document, and this can be compared to the encrypted hash, to determine the authenticity of the document & the digital signature.

To verify the identity of the signer and the digital signature, DSC or Digital Signature Certificate is issued. DSC is a secure digital public key that does all the decrypting & authenticates the identity of the holder. To understand what DSC is and why you require it, we'll delve into the details further in this article.

The underlying process here is far from simple, and it takes multiple algorithms carefully designed to encrypt, decrypt, and authenticate messages & data to create a digital signature. Here are a few of the most popular algorithms used for digital signatures.

**Features of Digital Signature**

- Digital signatures are used to authenticate the identity of the sender. It is like signing a message in electronic form.
- A digital signature is a protocol that produces the same effect as a real signature.
- It is a mark that only the sender can make and other people can easily recognize that it belongs to the sender. A digital signature is also used to confirm agreement to a message.
- A digital signature must be unforgeable and authentic.
- In a digital signature process, the sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination.
- If the result is true, the message is accepted otherwise it is rejected.
- A conventional signature is like a private key belonging to the signer of the document. The signer uses it to sign documents. The copy of the signature on a file is like a public key so anyone can use it to verify a document to compare it to the original signature

**Quest: - Digital Signature Certificate: Meaning, Types And Process.**

**Ans:-** India is moving digital and is likely to revamp its all documentation process from manual to digital. Digital signatures will form the basis of the same. Digital Signatures have already been granted legal status as per IT Act, 2000. It acts as evidence in the court of law across the country.

All electronic documents are incomplete without a digital signature. Just as any physical

document is incomplete without a signature or LTI (Left-hand Thumb Impression), similarly, all essential documents in electronic formats must have a digital signature of the applicant in place of the authorised signatory.

**Meaning**

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

Digital Signature Certificate (DSC) refers to a verified digital key that authenticates the sanctity of user data. Only the Certifying Authority (CA) can issue such a certificate. A DSC has vital information like Name, APNIC Account Name, your public key, Email Address, and Country of origin.

Once you receive a DSC, you can do away with manual physical documents. You can normally start entering into contracts with various business establishments using DSC. It almost works like an international ATM card that you can use anywhere across the globe for online transactions.

**Process for obtaining digital signature**

Digital Signature Certificate (DSC) Applicants can directly approach Certifying Authorities (CAs) with original supporting documents, and self-attested copies will be sufficient in this case

• DSCs can also be obtained, wherever offered by CA, using Aadhar eKYC based authentication, and supporting documents are not required in this case

• A letter/certificate issued by a Bank containing the DSC applicant's information as retained in the Bank database can be accepted. Such letter/certificate should be certified by the Bank Manager.

**Types**

The different types of Digital Signature Certificates are:

Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

**Importance of Digital Signature Certificate**

As its name suggests **Digital Signature Certificate** is an electronic signature that helps in validating the documents submitted through online mode. Today the world is rapidly growing towards digitization and everything is becoming online. Whether you want to pay your electricity bill or start a company everything can be done through the digitized modes. Earlier in order to put the electronic signature on a document the only way was to take the print of the document , put a sign and then send it back through by scanning. This was quite a time-consuming process considering which the DSC was introduced. **Digital Signature Certificate** is basically a kind of mathematical code that helps in authenticating the signature and keeping the data unaltered till it reaches its final destination. As far as the question about the importance of DSC is concerned the simple answer to this question is yes it is important to obtain the digital signature certificate in India. To throw more light on this statement through the course of this article we will be taking a looking at the multiple benefits of trademark registration.

**Ensures Safety** – As DSC is in electronic mode the chances of duplication of the certificate is practically negligible. Unlike the physical signatures it is not possible to alter, tamper or duplicate the certificate. There is a secure password that is handed over to the holder with which only he can take access of his signature. DSC makes the documents secured and legitimate.

**Reduced Time**– For putting the physical signature it is mandatory for the person to be present physically that may consume more time than required. Digital signatures make it seamless for the person to put his signature on the required documents from any place in the world and reduce the time taken in the whole procedure.

**Legal Validity**– The Digital Signature provides the legal validity to the documents and can be considered as evidence in the court of law. While submitting the documents with various departments for multiple registrations like company registration, IPR registration, Food licensing etc the food license is considered to be at par with the physical signature. In fact all the documents that are to be submitted on these online portals are required to be mandatorily authenticated with the use of the digital signature certificate.

**Cost Saving**– Apart from saving the excess time consumption digital signature certificate also save the various cost associated with the physical signature. Some of the costs which are saved with DSC include the costs of Ink, paper, printing, scanning, shipping, tracking and travelling etc.

**Make the procedures easier for clients**– It becomes very tiring for the client to check each documents, examine them physically and then either take a printout of all the documents or visit any place to put a sign on these documents. The concept of DSC allows the clients to do all of these at the comfort of their home simply by attaching the DSC to the required documents.

**Improved business operations**– As we have discussed in the above section DSC helps in reducing the time consumed, cost involved and is much more secure. All of these things help in reducing the time devoted by the employees in getting the documents signed and instead put them at the better use.

## UNIT: - FIVE

## Cyber Crimes under the IPC and IT Act

### Defining "Cyber Crimes"

The term "cyber-crimes" is not defined in any statute or rulebook. The word "cyber" is slang for anything relating to computers, information technology, internet and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality.

One finds laws that penalise cyber-crimes in a number of statutes and even in regulations framed by various regulators. The Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") penalise a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.

### Parallel Provisions in the IPC and IT Act

Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

***Hacking and Data Theft:*** Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both

It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "*whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description[1] for a term which may extend to 2 (two) years, or with fine, or with both.*" This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that "*whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.

***Receipt of stolen property:*** Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

***Identity theft and cheating by personation:*** Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Forgery has been defined in section 463 of the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment mat extend to 7 (seven) years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with

imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

***Obscenity:*** Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 (three) months, or with fine, or with both.